***Субіна Т. В.,***
*к.ю.н., старший науковий співробітник*
*Науково-дослідного центру з проблем оподаткування,*
*Національний університет ДПС України*

# СУСПІЛЬНІ ВІДНОСИНИ У СФЕРІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ОРГАНАХ ДПС УКРАЇНИ

Економічно розвинені країни вже усвідомили нагальну потребу у цілеспрямованому упорядкуванні інформаційних відносин і приймають необхідні законодавчі акти, які перебудовують діяльність органів влади, щодо державної інформаційної політики. І це зрозуміло, бо життя будь-якого суспільства – це удосконалення у структурах та в системах управління [1 с. 12].

Тісна співпраця між податківцями та громадянами можлива через інформаційні системи, які проводять форуми. Зокрема, ДПА України було видано наказ від 17.12.04 № 343-р «Про використання Інтернет-форуму ДПС України». Для досягнення цього на державному рівні було організовано роз'яснювальну роботу щодо особливостей, переваг і проблем, розвитку відкритого демократичного діалогу між усіма групами населення із залученням громадських формувань.

Великомасштабні заходи щодо реалізації таких програм необхідно починати тоді, коли можливості всього суспільства будуть мати відповідний інтелектуальний потенціал, а також будуть зрозумілими для всіх чи принаймні для більшості членів суспільства.

У державній податковій адміністрації та державних податкових інспекціях проводяться соціологічні опитування шляхом анкетування громадян і на web-сторінках щодо якості роботи з метою запобігання корупції органів державної податкової служби.

Опитування проводять під час проведення семінарів з платниками податків, відвідування громадянами (платниками податків) податкових органів тощо. У проведенні роботи з соціологічного опитування податковими службами беруть участь і волонтери податкової служби.

Аналізуючи засади адміністративно-правового регулювання у сфері податкових відносинах, що здійснюються через мережу Інтернет, необхідно звернути увагу і на деліктну поведінку окремих осіб.

На нашу думку, найбільш вразливою ланкою у сфері інформатизації є електронна пошта в органах ДПС України, яка має відкритий доступ до мережі Інтернет, податківець може отримати інформацію електронним листом на свою електронну пошту, а також без усяких перешкод зі свого робочого місця відіслати інформацію, дані, відомості в усі куточки світу.

Найбільшу небезпеку для суспільства, держави становить транскордонна організована кіберзлочинність: комп'ютерний тероризм, диверсії, інші прояви інформаційної боротьби кримінальних формувань із державою, правоохоронними органами; крадіжки інформації з комп'ютеризованих баз даних і порушення права інтелектуальної власності на комп'ютерні програми, шахрайства з використанням комп'ютерних технологій, особливо у сфері міжнародних економічних відносин (кредитно-фінансові, банківські) тощо [2, с. 178–179]. Окремі вчені наголошують уже не тільки на деліктній поведінці окремих осіб, а на так званих інформаційних війнах. Так, М. Требін зазначає, що інформаційна війна – це соціальне явище, що є однією з форм розв'язання існуючих різних суперечностей в усіх сферах суспільного життя між державами, націями, народами, спеціальними групами засобами інформаційного насильства. Метою інформаційної війни є забезпечення необхідного ступеня власної національної безпеки в усіх сферах суспільного життя і максимальне зниження рівня захищеності національної безпеки протидіючої сторони [3, с. 65].

На сьогодні в Україні недостатньо розроблені адміністративно-правові методики та тактики боротьби з комп'ютерними злочинами, злочинами в мережі Інтернет, що ускладнена трьома основними причинами:

– злочинні діяння мають місце у кіберпросторі (тобто злочини скоюються з використанням комп'ютерної чи комунікаційної мережі);

– міжнародні комп'ютерні мережі, такі як Інтернет, є відкритим середовищем, що дає можливість зловмисникам вчиняти певні дії за межами кордону, а правоохоронні органи повинні вчинити слідчі дії, обмежуючись територією власної держави. Таким чином, боротьбу із злочинами в мережі Інтернет не можна здійснювати без належного міжнародного співробітництва;
– відкритість глобальних інформаційних мереж надає можливість правопорушникам вибирати різні сфери для скоєння злочину.

Правопорушники можуть вибирати ті країни, у яких певні діяння, здійснені у кіберпросторі, не визначаються як адміністративні, кримінальні правопорушення, або в яких не розроблені ефективні процесуальні норми щодо боротьби зі злочинністю з використанням інформаційно-телекомунікаційних систем [4, с. 34–35].

Аналізуючи викладене, зазначимо, що при здійсненні злочину у мережі Інтернет правопорушник особисто не перебуває на місці злочину, чим і ускладнюється адміністративно-правове регулювання податкових відносин в інформаційній сфері.

Таким чином, забезпечення інформаційної безпеки в органах ДПС України щодо сфери застосування інформаційних технологій при виконанні нами завдань є одним із пріоритетних напрямів держави.

**Список використаної літератури**

1. Брижко В. До питання щодо гуманітарної інформатизації / В. Брижко // Правова інформатика. – 2003. – № 1. – С. 12.
2. Гриценко В. Організаційно-правові питання формування державної інформаційної політики України / В. Гриценко, В. Гавловський, В. Цимбалюк // Науковий вісник: збірник наукових праць Академії ДПС України. – 2002. – № 3 (17). – С. 178–180.
3. Требін М. Інформаційне суспільство, війни нової епохи / М. Требін // Віче. – 2002. – № 4 (121). – С. 65.
4. Бутузов В. М. Специфіка протидії комп'ютерній злочинності / В. М. Бутузов // Організаційно-правове забезпечення електронного оподаткування: збірник тез. – Ірпінь: Національний університет державної податкової служби України, 2008. – С. 34–35.